

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE: EMJ 3/13/24

Amey
3/13/24

UNITED STATES DISTRICT COURT

WESTERN

for the
DISTRICT OF

OKLAHOMA

In the Matter of the Search of)

Cell phone associated with phone)

Number: 405-613-9147)

Case No: MJ-24- 224- AMG

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2252A(a)(5)(B)

18 U.S.C. § 2252A(a)(2)

Offense Description

Possession of Child Pornography

Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Marisol Flores, Federal Bureau of Investigations, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

Marisol Flores
Special Agent
Federal Bureau of Investigations

Sworn to before me and signed in my presence.

Date:

3/13/2024



Judge's signature

City and State: Oklahoma City, Oklahoma

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge

Printed name and title

**THE UNITED STATES DISTRICT COURT FOR THE WESTERN
DISTRICT OF OKLAHOMA**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Marisol Flores, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since May 2015, and I am currently assigned to the Oklahoma City Division. Since joining the FBI, I have been involved in investigations of child exploitation matters and computer crimes against children. I am currently assigned to investigate violations of federal law involving the exploitation of children. I have gained expertise in conducting such investigations through in-person trainings, classes, and everyday work in my current role as an SA with the FBI.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the online activities of Michael Rios¹, who is believed to use a cell phone with assigned phone number 405-613-9147 (the "SUBJECT DEVICE,"

¹ In August of 2012, in Oklahoma County, Rios was charged with several criminal charges to include rape in the first degree by instrumentation and indecent or lewd acts with a child under sixteen. Rios was acquitted of these charges, and all the associated charges, in 2013 by a jury trial. In November of 2022, in Oklahoma County, Rios was charged with indecent or lewd acts with a child under sixteen and possession of obscene material involving the participation of a minor under the age of eighteen. In November of 2023, the indecent or lewd acts with a child under sixteen was amended to manufacturing child pornography. Rios is currently awaiting trial for these charges.

as further described in Attachment A). As shown below, there is probable cause to believe that Michael Rios (Rios) possessed child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and distributed child pornography in violation of 18 U.S.C. § 2252A(a)(2). I submit this Application and Affidavit in support of a search warrant authorizing a search of the SUBJECT DEVICE. Located within the SUBJECT DEVICE, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, specifically Rios' cell phone in which he uses to communicate with other individuals, to include an undercover law enforcement officer, for the purposes of accessing, viewing, and distributing child pornography. I request authority to search the entire SUBJECT DEVICE.

4. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the foregoing violations are presently located on the SUBJECT DEVICE.

BACKGROUND OF THE INVESTIGATION

5. Between on or about January 8, 2024, and January 9, 2024, an FBI Online Covert Employee (OCE), who is a member of the FBI Birmingham Division's Child Exploitation and Human Trafficking Task Force in Birmingham, Alabama, was connected to the Internet in an online undercover capacity. The OCE accessed two private channels

on the Signal Application.² These private channels, within the Signal Application, were dedicated to users who have a sexual interest in children. The private channels were by invite only and each user had to be provided a specific link to gain access to the channels. Users within the channels were openly sharing Child Sexual Abuse Material (CSAM) amongst one another in an open forum style of setting. During a covert online session, Signal User: "Harry +1 405-613-9147" distributed four videos within the private channel titled "Babysex," which depicted CSAM. The videos were distributed to the group on January 8, 2024, at or around 12:32 PM. One of the videos can be described as follows:

CFE11EDD-95B9-44F6-87A7-42C95E710B25.MP4

25 seconds in length

Description: The video depicts a prepubescent female in a bathtub. The child is holding an adult, erect penis in both her hands while putting her mouth on and sucking the penis. The child pulls away from the penis and looks up. At that time, a hand enters the screen and gestures for the child to resume the oral sex. Then the hand is placed on the child's head as the child is forced into continuing the oral sex.

² The Signal application is an encrypted messaging service for instant messaging, voice, and video calls. The instant messaging function includes sending text, voice notes, images, videos, and other files through a secured transmission. Communication may be one-to-one between users, through direct messaging, or for group messaging in larger private channels. Signal is a free, privacy-focused messaging and voice talk app you can use on Apple and Android smartphones, and via desktop. Communications on Signal are end-to-end encrypted, which keeps the content of communications between users secure from the company's view. An active phone number is needed to create a new account.

During another covert online session, Signal User: "Harry +1 405-613-9147" distributed nineteen images, ten of which depicted CSAM, within the private channel titled "Grupo sin límites." The images were distributed to the group on January 9, 2024, at or around 10:08 PM. Two of the images can be described as follows:

One image depicts two minor females standing in front of a white wall. Both minor children are naked exposing their vaginas. One child has dark brown hair and is covering her chest area with her hands. The other child has her breast exposed with her hands behind her back.

The other image has a minor female squatting on a brown table and there is a red backdrop behind her. The child has on white net hose on her legs and is wearing white shoes. There is white lace around her pelvic area, with the letters "OK" on the lace. The child's vagina is exposed, and she is not wearing any additional clothing. On the left hand of the photo is script, "for Pollyfan".

6. On or about February 8, 2024, an administrative subpoena was served to T-Mobile requesting subscriber information for assigned telephone number 405-613-9147. On or about February 9, 2024, T-Mobile provided the following results:

Customer Name: Michael Rios

Subscriber Name: Michael Rios

Service Address: 2927 SW 55th St., Oklahoma City, OK 73119 USA

Billing Address: 2927 SW 55th St., Oklahoma City, OK 73119 USA

Start Time: Jul 21, 2023 07:00:00 (UTC)

End Time: Jan 01, 0001 08:00:00 (UTC)

7. On March 7, 2024, physical surveillance observed a gray Ford F-250, bearing Oklahoma license plate NTY-146, depart 2308 County Road 1280, Blanchard, Oklahoma, 73010. This vehicle is registered to Michael Rios at 2927 SW 55th St., Oklahoma City, Oklahoma. Rios was identified as the driver of the Ford F-250 bearing Oklahoma license plate NTY-146. During surveillance, Rios and his vehicle were observed at a construction work site. While physical surveillance was observing Rios, a phone call from law enforcement was made to the Signal Application user "Harry +1 405-613-9147" at phone number 405-613-9147. At the time the phone call was made, Rios was observed walking over to where he had left his phone,³ then picked up the phone, touched the phone, and then set the phone back down where he had it. This coincided with law enforcement hearing phone ringing and then an automated voicemail, while having dialed Signal Application user "Harry +1 405-613-9147," at phone number 405-613-9147.

8. Based on my training and experience, individuals who possess and distribute CSAM will use multiple devices to store and access their collection of CSAM. With Rios identified as the T-Mobile subscribed customer to phone number 405-613-9147 and addressing his cell phone during a phone call made by law enforcement to phone number 405-613-9147, I believe Rios uses the SUBJECT DEVICE with assigned phone number 405-613-9147. Therefore, I believe Rios is the Signal Application user "Harry +1 405-613-9147," who possessed and distributed CSAM, and I am seeking authorization to search the

³ Prior to the phone call made by law enforcement, Rios was observed by physical surveillance on this cell phone. Rios had placed the cell phone on bricks which were on top of a scaffolding structure prior to the phone call made by law enforcement.

SUBJECT DEVICE where Rios is likely storing CSAM.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text based online communications such as Internet forums and email.

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child Sexual Abuse Material" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

d. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include

encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. “Sexually explicit conduct” applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. Section 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. Section 2256 (8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c)

masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* U.S.C. § 2256(2)(A).

k. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

m. A “storage medium” or “storage device” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

n. A “website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

10. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is

difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

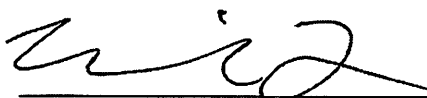
11. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child sexual abuse material where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

12. Finally, I know that many cell phones, can be encrypted by the user using his finger and/or thumbprint or facial image to lock and unlock the device. Without the user's prints, the devices are difficult, if not impossible, for law enforcement personnel to unlock. Accordingly, I am requesting that, to the extent law enforcement seizes the SUBJECT DEVICE described in Attachment A, and if such device features such encryption, then law enforcement may, while executing the search warrant of the SUBJECT DEVICE, use Rios'

finger and/or thumbprint and/or facial image with any such encryption feature to attempt to unlock the device.

CONCLUSION

13. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that Michael Rios, while using the SUBJECT DEVICE, possessed child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and distributed child pornography in violation of 18 U.S.C. § 2252A(a)(2). Additionally, there is probable cause to believe that evidence of the criminal offenses is located on the SUBJECT DEVICE, and this evidence, listed in Attachment B to this Affidavit, incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses. As described in the probable cause section, there is probable cause to believe Michael Rios violated the aforementioned statutes. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.



MARISOL FLORES
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Signed and sworn before me this 13th day of
March, 2024.



AMANDA MAXFIELD GREEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF THE SUBJECT DEVICE

- **Cell phone associated with phone number: 405-613-9147**

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Contraband, evidence, fruits, and instrumentalities related to Rios distributing child pornography in violation of 18 U.S.C. § 2252A(a)(2) or possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), in any form, including, but not limited to:

1. Any and all notes, documents, records, or correspondence, in digital format and medium pertaining to the violations described in the affidavit.

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all notes, documents, records, or correspondence, in digital format or medium identifying persons involved in violations described in the affidavit.

6. Any and all notes, documents, records, or correspondence, in digital format or medium concerning the violations described in the affidavit.

7. Any and all notes, documents, records, or correspondence, in digital format or medium concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in digital format or medium concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in digital format or

medium that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

10. Any and all visual depictions of minors engaging in sexually explicit conduct.

11. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in digital format or medium pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

If the smart cell phone, as described herein, is found that requires access by using a finger or thumbprint or facial recognition to unlock the device, then, while executing the search warrant of the SUBJECT DEVICE, a law enforcement officer may press the finger or thumbprint of Michael Rios onto the device to try to unlock it or use their face to unlock the device via facial recognition.